UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/519,239	01/23/2006	Thomas Fountain	200634-0109-00-US (425596	9717

23973 7590 12/08/2010
DRINKER BIDDLE & REATH
ATTN: INTELLECTUAL PROPERTY GROUP
ONE LOGAN SQUARE, SUITE 2000
PHILADELPHIA, PA 19103-6996

EXAMINER	
CHEN, SHIN HON	
ART UNIT	**PAPER NUMBER**
2431	

NOTIFICATION DATE	DELIVERY MODE
12/08/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

DBRIPDocket@dbr.com
penelope.mongelluzzo@dbr.com

Office Action Summary	Application No.	Applicant(s)
	10/519,239	FOUNTAIN ET AL.
	Examiner	Art Unit
	SHIN-HON CHEN	2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 September 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-66* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-66* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 December 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *6/28/10 and 8/13/10*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-66 have been examined.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9/13/10 has been entered.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 6/28/10 and 8/13/10 are being considered by the examiner.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Berson et al. U.S. Pat. No. 7051199 (hereinafter Berson) in view of Howard, JR, et al. U.S. Pub. No. 20020126849 (hereinafter Howard).

6. As per claim 1, Berson discloses a cryptographic key server suitable for providing cryptographic services to remote devices coupled to said cryptographic key server via a network (Berson: column 3 lines 3-5), said cryptographic key server comprising: a secure network interface engine executing on said cryptographic key server (Berson: column 5 lines 44-67; column 9 lines 40-50), said secure network interface engine operable: to establish a secure network communication channel with at least one remote device (Berson: column 3 lines 5-8: establish secure channel); to unmarshal secured cryptographic service requests received from said at least one remote device (Berson: column 10 lines 14-21); and to marshal and transmit secure cryptographic service responses to said at least one remote device (Berson: column 10 lines 14-21); and a cryptographic service engine executing on said cryptographic key server, said cryptographic service engine being in bi-directional communication with said secure network interface engine, said cryptographic service engine operable to provide cryptographic services requested by said at least one remote device via said secure network interface engine (Berson: column 3 lines 14-26: providing cryptographic services), wherein said cryptographic service requests comprise input data to be transformed; at least one unique identifier for identifying at least one key for performing the transformation; and instructions for how the cryptographic service engine should transform the data (Berson: column 10 lines 40-57).

Berson discloses providing key from remote device to cryptographic key server via secure network for cryptographic operation to reduce processing burden on the remote device. Berson does not explicitly disclose providing key through key escrow to prevent storing keys together with protected data to ensure data security. However, Howard discloses method of r managing key material in cryptographic assets that allows a key escrow server to provide keys to cryptographic services upon authorization by user (Howard: [0017] and [0050]). It would have been obvious to one having ordinary skill in the art to store cryptographic keys in an escrow key server/provider instead of locally on a remote device and providing cryptographic key material to appropriate cryptographic asset/service upon authorization because both discloses method of protecting data in distributed network environment through use of trusted third party security system. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Howard within the system of Berson because it provide secure storage and management of cryptographic keys.

7. As per claim 2, Berson as modified discloses the cryptographic key server as recited in claim 1. Berson further discloses wherein said at least one device is an application server (Berson: column 12 lines 46-63: the request can be generated from any computing mechanism).

8. As per claim 3. Berson as modified discloses the cryptographic key server as recited in claim 1. Berson further discloses wherein said secure network interface engine is arranged such that said secure network communication channel is established according to a Secure Socket Layer (SSL) protocol (Berson: column 3 lines 5-8: secure tunnel; column 11 lines 34-36).

9. As per claim 4, Berson as modified discloses the cryptographic key server as recited in claim 1. Berson further discloses wherein said secure network interface engine is arranged such

that said secure network communication channel is established according to a Transport Layer Security (TLS) protocol (Berson: column 3 lines 5-8).

10. As per claim 5, Berson as modified discloses the cryptographic key server as recited in claim 1. Berson further discloses wherein said secure network interface engine supports multiple communications protocols including a Secure Socket Layer (SSL) protocol and a Transport Layer Security (TLS) protocol, said secure network interface engine being responsive to said at least one device to establish said secure network communication channel according to a protocol selected by said at least one device (Berson: column 3 lines 5-8: establishing tunnel between two devices allows secure communication between them based on well known communication protocols).

11. As per claim 6, Berson as modified discloses the cryptographic key server as recited in claim 1. Berson further discloses wherein said cryptographic service engine and said secure network interface engine are components of a single process executing on said cryptographic key server (Berson: column 9 lines 40-60).

12. As per claim 7, Berson as modified discloses the cryptographic key server as recited in claim 1. Berson further discloses wherein said cryptographic service engine is operable to perform encryption and decryption functions (Berson: column 6 lines 59-66).

13. As per claim 8, Berson as modified discloses the cryptographic key server as recited in claim 7. Berson further discloses wherein said encryption and decryption functions comprise: symmetric block ciphers; generic cipher modes; stream cipher modes; public-key cryptography; padding schemes for public-key systems; key agreement schemes; elliptic curve cryptography; one-way hash functions; message authentication codes; cipher constructions based on hash functions; pseudo random number generators; password based key derivation functions; Shamir's secret sharing scheme and Rabin's information dispersal algorithm (IDA); DEFLATE (RFC 1951) compression/decompression with gzip (RFC 1952) and zlib (RFC 1950) format support; fast multi-precision integer (bignum) and polynomial operations; finite field arithmetic, including GF(p) and GF(2.sup.n); and prime number generation and verification (Berson: column 5 lines 44-67; column 6 lines 44-67).

14. As per claim 9, Berson as modified discloses the cryptographic key server as recited in claim 7. Berson further discloses wherein said encryption and decryption functions comprise: DES, 3DES, AES, RSA, DSA, ECC, RC6, MARS, Twofish, Serpent, CAST-256, DESX, RC2, RC5, Blowfish, Diamond2, TEA, SAFER, 3-WAY, Gost, SHARK, CAST-128, Square, Shipjack, ECB, CBC, CTS, CFB, OFB, counter mode(CTR), Panama, ARC4, SEAL, WAKE, Wake-OFB, Blumblumshub, ElGamal, Nyberg-Rueppel (NR), Rabin, Rabin-Williams (RW), LUC, LUCELG, DLIES (variants of DHAES), ESIGN padding schemes for public-key systems: PKCS#1 v2.0, OAEP, PS SR, IEE P1363 EMSA2, Diffie-Hellman (DH), Unified Diffie-Hellman (DH2), Menezes-Qu-Vanstone (MQV), LUCDIF, XTR-DH, ECDSA, ECNR, ECIES, ECDH, ECMQV, SHA1, MD2, MD4, MD5, HAVAL, RIPEMD-160, Tiger, SHA-2 (SHA-256,

SHA-384, and SHA-512), Panama, MD5-MAC, HMAC, XOR-MAC, CBC-MAC, DMAC, Luby-Rackoff, MDC, ANSI X9.17 appendix C, PGP's RandPool, PBKDF1 and PBKDF2 from PKCS #5 (Berson: column 5 lines 44-67; column 6 lines 44-67).

15. As per claim 10, Berson as modified discloses the cryptographic key server as recited in claim 1. Berson further discloses wherein said cryptographic service engine is operable to perform signing and verifying functions (Berson: column 8 lines 17-55).

16. As per claim 11, Berson as modified discloses the cryptographic key server as recited in claim 10. Berson further discloses wherein said signing and verifying operations includes RSA and DSA (Bersson: column 8 lines 17-55).

17. As per claim 12, Berson as modified discloses the cryptographic key server as recited in claim 1. Berson further discloses wherein said cryptographic service engine is operable to perform hashing operations (Berson: column 5 lines 44-67).

18. As per claim 13, Berson as modified discloses the cryptographic key server as recited in claim 10. Berson further discloses wherein said hashing operations includes HMAC with SHA-1 (Berson: column 6 lines 44-67).

19. As per claim 14, Berson as modified discloses the cryptographic key server as recited in claim 1. Berson further discloses wherein said cryptographic service engine is further operable to

authenticate and to determine authorization of a request for cryptographic services prior to and as a condition of performing said cryptographic services (Berson: column 8 lines 36-55).

20. As per claim 15, Berson as modified discloses the cryptographic key server as recited in claim 14. Berson further discloses wherein authenticating a request for cryptographic services includes verifying an identity of one or more of a set comprising: a client that is requesting for cryptographic services; said at least one remote device from which said client requesting for cryptographic services; a function or program that is executing on said at least one remote device (Berson: column 8 lines 36-55).

21. As per claim 16, Berson as modified discloses the cryptographic key server as recited in claim 14. Berson further discloses wherein determining authorization of a request for cryptographic services includes determining authorization privileges granted to one or more of a set comprising: a client that is requesting for cryptographic services; said at least one remote device from which said client requesting for cryptographic services; a function or program that is executing on said at least one remote device (Berson: column 8 lines 36-55).

22. As per claim 17, Berson as modified discloses the cryptographic key server as recited in claim 16. Berson further discloses wherein the operation of determining authorization a request for cryptographic services further includes determining whether said request for cryptographic services is within the privileges of a requestor that is associated with said request for cryptographic services (Berson: column 8 lines 36-55).

23. As per claim 18, Berson as modified discloses cryptographic key server as recited in claim 1. Berson further discloses wherein said cryptographic service engine is operable to track requests for cryptographic services (Berson: column 16 lines 48-61).

24. As per claim 19, Berson as modified discloses the cryptographic key server as recited in claim 1. Berson further discloses said cryptographic key server further comprising: a private key engine, said private key engine operable to provide private keys for use by said cryptographic service engine in performing cryptographic services (Berson: column 10 lines 5-13: key may be stored in database/private key engine).

25. As per claim 20, Berson as modified discloses the cryptographic key server as recited in claim 1. Berson further discloses wherein said cryptographic key server is a network security appliance (Berson: column 8 lines 58-67).

26. As per claim 21, Berson as modified discloses the cryptographic key server as recited in claim 1. Berson further discloses wherein said cryptographic key server has a computer hardware architecture supporting said cryptographic service engine and said secure network interface engine, said computer hardware architecture comprising: a databus; a central processing unit bi-directionally coupled to said databus; a persistent storage device bi-directionally coupled to said databus; a transient storage device bi-directionally coupled to said databus; a network I/O device bi-directionally coupled to said databus; a cryptographic accelerator card bi-directionally coupled

to said databus; a hardware security module bi-directionally coupled to said databus and suitable for storing private keys; and a smart card interface device (Berson: column 6 lines 44-67).

27. As per claim 22, Berson as modified discloses the cryptographic key server as recited in claim 21. Berson further discloses wherein said hardware security module is a tamper resistant device (Berson: column 6 lines 44-67).

28. As per claim 23, Berson as modified discloses the cryptographic key server as recited in claim 21. Berson further discloses wherein said private keys are loaded into said hardware security module and stored in an encrypted format (Berson: column 3 lines 14-21).

29. As per claim 24, Berson as modified discloses the cryptographic key server as recited in claim 21. Berson further discloses wherein said private keys are loaded into said hardware security module via a smart card storing said encrypted private keys (Berson: column 6 lines 44-67).

Claim Rejections - 35 USC § 103

30. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

31. Claims 25-66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Berson in view of Howard and further in view of Juels et al. U.S. Pub. No. 20040030932 (hereinafter Juels).

32. As per claim 25, Berson as modified discloses the cryptographic key server as claim 24. Berson does not explicitly disclose applying secret sharing scheme for cryptographic service. However, Juels discloses secret sharing scheme during network communication to ensure cryptographic process is secure (Juels: [0008] and [0116]). It would have been obvious to one having ordinary skill in the art to use secret sharing cryptographic scheme when multiple clients interface with a security server for cryptographic communication. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Juels within the system of Berson because it enhances the security of cryptographic keys.

33. As per claim 26-66 claims 26-66 encompass the same or similar scope as claims 1-25. Therefore, claims 26-53 are rejected based on the same reason set forth above in rejecting claims 1-25.

Response to Arguments

34. Applicant's arguments with respect to claims 1-66 have been considered but are moot in view of the new ground(s) of rejection.

35. Applicant is advised to amend all independent claims to incorporate limitations of claim 1 to more precisely disclose the inventive concept to expedite prosecution. Applicant is welcome to contact the examiner to accelerate prosecution.

Conclusion

36. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Murty et al. U.S. Pub. No. 20030084290 discloses distributed security architecture for storage area networks.

Wong et al. U.S. Pub. No. 20020101998 discloses fast escrow delivery.

Hamid et al. U.S. Pat. No. 7191466 discloses method of user authentication for password based system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHIN-HON CHEN whose telephone number is (571)272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shin-Hon Chen
Primary Examiner
Art Unit 2431

/Shin-Hon Chen/
Primary Examiner, Art Unit 2431